Audit Report

APPLICATION OF YEAR 2000 LESSONS LEARNED

Report No. D-2001-175

August 22, 2001

Office of the Inspector General
Department of Defense

Report Documentation Page

Report Date 22Aug2001	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Application of Year 2000 Lessons Learned	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Report Number** D-2001-175
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract

During the late 1990s, DoD Components applied extensive efforts and expended significant resources towards preparing for the year 2000 conversion. As shown in the Office of Management and Budget 11 th Quarterly Progress Report, "Department of Defense Status of Year 2000 Efforts," November 15, 1999, DoD tracked 2,367 mission-critical and 7,267 nonmission-critical systems. The DoD also operated 637 military installations around the world and in the United States and relied on supporting infrastructure systems that were also vulnerable to year 2000 problems. In addition, the DoD had 15 centralized mainframe computer sites comprising 351 computer domains in operation on January 1, 2000. More than one-third of the Federal Government's mission-critical systems were in the DoD. The DoD year 2000 challenge represented a substantial undertaking in scope, magnitude, and complexity that far exceeded any other Federal department. The enormous efforts that DoD undertook to ensure year 2000 readiness were largely successful. Since January 1, 2000, the common theme of year 2000 lessons learned by both the private and public sectors has been the in-depth awareness by managers and users of an organization's dependency on information technology and of the interdependencies among organizations, commercial vendors, and systems.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 38	

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
DISA	Defense Information Systems Agency
DOT&E	Director, Operational Test and Evaluation
PSA	Principal Staff Assistant
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2885

August 22, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Audit Report on Application of Year 2000 Lessons Learned (Report No. D-2001-175)

We are providing this audit report for review and comment. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all unresolved issues be resolved promptly. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comments for recommendation 1 were partially responsive. Therefore, we request additional comments on recommendation 1. Additionally, completion dates are needed for all recommendations. We request management provide the comments and dates by September 20, 2001.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Ms. Wanda A. Hopkins at (703) 604-9049 (DSN 664-9049) (wahopkins@dodig.osd.mil) or Ms. Virginia G. Rogers at (703) 604-9041 (DSN 664-9041) (vrogers@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-175 **August 22, 2001**
(Project No. D2001AS-0006)

Application of Year 2000 Lessons Learned

Executive Summary

Introduction. During the late 1990s, DoD Components applied extensive efforts and expended significant resources towards preparing for the year 2000 conversion. As shown in the Office of Management and Budget 11th Quarterly Progress Report, "Department of Defense Status of Year 2000 Efforts," November 15, 1999, DoD tracked 2,367 mission-critical and 7,267 nonmission-critical systems. The DoD also operated 637 military installations around the world and in the United States and relied on supporting infrastructure systems that were also vulnerable to year 2000 problems. In addition, the DoD had 15 centralized mainframe computer sites comprising 351 computer domains in operation on January 1, 2000. More than one-third of the Federal Government's mission-critical systems were in the DoD. The DoD year 2000 challenge represented a substantial undertaking in scope, magnitude, and complexity that far exceeded any other Federal department. The enormous efforts that DoD undertook to ensure year 2000 readiness were largely successful. Since January 1, 2000, the common theme of year 2000 lessons learned by both the private and public sectors has been the in-depth awareness by managers and users of an organization's dependency on information technology and of the interdependencies among organizations, commercial vendors, and systems.

Objectives. Our objective was to assess how widely and successfully the DoD had applied the lessons learned from the year 2000 conversion experience to other information technology programs and management issues.

Results. Since the year 2000 rollover, many DoD Components adapted management experiences gained from the year 2000 conversion and reused and updated data compiled during those efforts, such as system inventories, thin-lines, contingency plans, and configuration management. The reuse of data and adaptation of management experiences were largely driven by individual actions within the DoD Components and not by the DoD Chief Information Officer. As a result, the DoD Components initiated and took commendable but varied steps to use year 2000 lessons learned in managing their information technology systems, whereas the DoD Chief Information Officer missed opportunities to readily lead the way in managing information assurance and information technology investments (finding A).

The DoD Chief Information Officer had not readily adapted year 2000 experiences to managing information assurance and information technology investments. As a result, the task of responding to congressional and Office of Management and Budget requirements for ensuring that systems and networks are reasonably secure, particularly with respect to the Government Information Security Reform requirements, and for complying with the Clinger-Cohen Act, has been made even more difficult (finding B).

Summary of Recommendations. We recommended that the Chief Information Officer, DoD, establish a written DoD management plan for information assurance compliance that will oversee the certification and accreditation process required by DoD Instruction 5200.40 and respond to the requirements of Government Information Security Reform. We also recommended that the Chief Information Officer, DoD, assess the cost-effectiveness of purchasing new licenses for analysis and renovation tools to use in detecting defects or abnormalities in software; implement a mission or business area approach for managing information technology investments in accordance with the Clinger-Cohen Act and DoD Directive 5000.1; and implement an oversight process for complete repair, retirement, or replacement of systems that used date-windowing techniques during the year 2000 conversion process.

Management Comments. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the findings and recommendations, stating that management directed the Government Information Security Reform Integrated Process Team to develop a plan for Government Information Security Reform implementation that leveraged the assessment mechanism from the Defense Information Technology Security Certification and Accreditation Process. Management will also continue to assess the commercial market for analysis and renovation tools, and will consider publishing guidelines to assist in determining the best mix of tools. Additionally, the Deputy Chief Information Officer will undertake a thorough review and reengineering of information technology investment and acquisition oversight. The new information technology management and oversight concept includes portfolios and families of systems reviews, which are a mission or business area approach to managing information technology. A discussion of management comments is located at finding B of the report and the complete text is in the management comments section.

Audit Response. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) comments were responsive except for comments on the DoD management plan. The implementation plan developed by the Government Information Security Reform Integrated Process Team primarily focuses on the Government Information Security Reform requirements for FY 2001. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) should also have a DoD management plan that oversees and provides guidance on the certification and accreditation of information systems and networks, using the DoD information technology registry as the starting point. We request that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide additional comments by September 20, 2001.

Table of Contents

Executive Summary

Introduction

Findings

Appendixes

Management Comments

Background

Year 2000 Conversion Efforts. During the late 1990s, DoD Components applied extensive efforts and expended significant resources towards preparing for the year 2000 (Y2K) conversion. DoD spent an estimated $3.6 billion in its efforts to accomplish Y2K conversion, monitor activities during the rollover and leap year, and react to the problems that did occur. The DoD portion was about 44 percent of the total amount that the Federal Government spent on Y2K efforts.

The scope and complexity of the Y2K problem for DoD was unparalleled in the Federal Government. As shown in the Office of Management and Budget 11th Quarterly Progress Report, "Department of Defense Status of Year 2000 Efforts," November 15, 1999, DoD tracked 2,367 mission-critical and 7,267 nonmission-critical systems. The DoD also operated 637 military installations around the world and in the United States and relied on supporting infrastructure systems that were also vulnerable to Y2K problems. In addition, the DoD had 15 centralized mainframe computer sites comprising 351 computer domains in operation on January 1, 2000. More than one-third of the Federal Government's mission-critical systems were in the DoD. The DoD Y2K challenge represented a substantial undertaking in scope, magnitude, and complexity that far exceeded any other Federal department.

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C^3I)] serves as the DoD Chief Information Officer (CIO). By using the system inventory and interdependency data, establishing an overall DoD Year 2000 Management Plan, and working through the Senior Steering Group, the DoD CIO played a prominent role in managing the progress of the Y2K conversion effort. The Deputy Secretary of Defense chaired monthly DoD Y2K Steering Group meetings to review progress toward achieving readiness for Y2K. Participants of the meetings included senior DoD leaders, such as the Under Secretaries of Defense; Service Under Secretaries; Vice Chief of Staff of the Army; Vice Chief of Naval Operations; Assistant Commandant of the Marine Corps; Director, Operational Test and Evaluation; Principal Staff Assistants from the Office of the Secretary of Defense; DoD agency CIOs; and Joint Staff representatives. The final Senior Steering Group meeting was held on February 9, 2000.

The enormous efforts that DoD undertook to ensure Y2K readiness were largely successful. For example, only 61 out of 1,059 logistics systems experienced notable failures during or following January 1, 2000. Of the 61 systems with failures, 60 were nonmission-critical systems that did not go through end-to-end testing. Technicians were able to correct the Y2K problem for the one mission-critical system, the Streamlined Automated Logistics Transmission System, within hours of the failure because of their experience with a near-identical problem during Y2K testing.

Principal Staff Assistants. The Principal Staff Assistants (PSAs) for the Office of the Secretary of Defense report directly to the Secretary or the Deputy Secretary of Defense and are responsible for their respective business functional processes such as health affairs, personnel, communications, logistics, and weapon systems. During the Y2K conversion, the PSAs were responsible for coordinating the end-to-end testing for their respective business function processes. The PSAs also had various oversight responsibilities for their community systems. For example, the PSA for Communications served as the Office of the Secretary of Defense (C^3I) Y2K coordinator and oversaw approximately 600 mission-critical and 500 mission-essential systems.

Lesson Learned Reports. Since January 1, 2000, the common theme of Y2K lessons learned by both the private and public sectors has been the in-depth awareness by managers and users of an organization's dependency on information technology and of the interdependencies among organizations, commercial vendors, and systems. Report 106-244 from the FY 2000 DoD Appropriations Bill directed DoD to provide a report to the congressional Defense committees by March 15, 2000, on Y2K lessons learned, emphasizing which additional programs should be continued and what lessons could be applied to information assurance. The ASD(C^3I), Air Force, and Joint Staff prepared reports on Y2K lessons learned, while the Navy provided an undated document. See Appendix A for audit coverage by the Air Force, Army, and Navy on Y2K lessons learned.

Department of Defense. The ASD(C^3I) report, dated March 15, 2000, detailed the DoD efforts to ensure Y2K readiness and identified the most important lessons to be used in future efforts to secure information infrastructures. Lessons learned, applicable to DoD and other Federal agencies, included an increased awareness of the need to cooperate on cross-cutting issues, the dependence on information technology systems, and the importance of computer professionals. The lessons learned for CIOs included the importance of partnerships, centralized guidance with decentralized execution, and an accurate inventory of information technology. According to the ASD(C^3I) report, the DoD lessons learned provide a roadmap for improving information technology management, and the DoD CIO would monitor their implementation.

Air Force. According to the Air Force Year 2000 Final Report, the Air Force collected more than 400 Y2K lessons learned suggestions from the Major Commands, Direct Reporting Units, and Field Operating agencies. The Air Force consolidated the suggestions into 60 lessons and recommendations. Some key lessons learned included the need for improved resource management, including configuration management, procuring independent verification and validation tools, implementing code-scanning processes, a comprehensive information technology infrastructure database, and operational and system architectures at the mission level.

Joint Staff. Volume One of the Joint Staff Year 2000 Campaign Plan summarizes 12 lessons learned that were presented to the Deputy Secretary of Defense by the Joint Staff Y2K Task Force Leader. The lessons included reusing data compiled for Y2K efforts for other information technology issues, incorporating information technology issues into routine exercises and training, and developing a prototype Joint Operational Architecture. According to the Year 2000 Campaign Plan, the results of, and lessons learned from, the Y2K conversion process were to be maintained and used in future endeavors.

Navy. The Navy provided an undated document on Y2K lessons learned that stated that Navy Fleet, Systems Command, and Major Claimant representatives met to review the reasons for the success with Y2K conversion and to capitalize on the Navy investment of resources for Y2K preparations. The document summarized the key findings and presented recommendations for improvements in future information systems management. Some of the key recommendations included broadening the duties and responsibilities of the Navy CIO, establishing a methodology for obtaining and maintaining current configuration information, and continuing the development and expansion of land-based laboratory interoperability testing. The document stated that steps were already underway to implement some of the recommendations. Furthermore, the document recommended that, as an enterprise, the Navy should embrace those initiatives and leverage the Y2K lessons learned to meet information technology challenges.

Objectives

Our objective was to assess how widely and successfully DoD applied the lessons learned from the Y2K conversion to other information technology programs and management issues. See Appendix A for a discussion of the audit scope and methodology.

A. Application of Year 2000 Lessons Learned

Since the year 2000 rollover, many DoD Components adapted management experiences gained from the Y2K conversion and reused and updated data compiled during those efforts, such as system inventories, thin-lines, contingency plans, and configuration management. The reuse of data and adaptation of management experiences were largely driven by individual actions within the DoD Components and not by the DoD CIO. As a result, the DoD Components initiated and took commendable and varied steps to use Y2K lessons learned in managing their information technology systems, whereas the DoD CIO missed opportunities to readily lead the way in managing information assurance and information technology investments. (Finding B discusses these missed opportunities.)

Reuse of Year 2000 Inventory Database

The FY 2001 DoD Authorization Act Section 811, "Acquisition and Management of Information Technology," requires the DoD CIO to maintain an inventory of DoD mission-critical and mission-essential information systems. In addition, section 811 requires identification of interfaces between the registered systems and other information systems and the development and maintenance of contingency plans for the systems registered with the DoD CIO. Section 811 requires registration information to be updated quarterly and requires each system to have an appropriate information assurance strategy as determined by the CIO. Section 811 prohibits awarding any contract for any system not registered with the DoD CIO. Section 811 supersedes section 8121, "Certifications as to Compliance with the Clinger-Cohen Act," of the FY 2000 DoD Appropriations Act. The DoD CIO and DoD Components provided examples of reusing the Y2K inventory database for section 811 registration. However, the DoD Information Technology Registry, used for section 811 registration, records only whether the system has interfaces. According to DoD CIO representatives, ASD(C^3I) relies on other databases, such as at the Component level, to identify the specific interface.

Principal Staff Assistants

The communications, financial, health affairs, logistics, and personnel communities applied Y2K lessons learned to include the reuse of data, management structure, configuration management, and end-to-end testing. However, the number and types of lessons learned that were applied varied among the PSAs.

Under Secretary of Defense (Comptroller). In 2000, the DoD Chief Financial Officer (CFO) began efforts to institute a Y2K-type management approach to the DoD Financial and Feeder Systems Compliance Process, which entailed the implementation of a similar five-phased approach for ensuring that DoD critical finance, accounting, and feeder systems meet Federal financial management requirements. The process, which was recommended by the Inspector General, DoD, and endorsed by the General Accounting Office, includes lessons learned from the year 2000 such as:

- requiring senior leadership involvement,
- defining criticality of systems,
- identifying required interfaces for all Components' critical feeder systems and the Defense Finance and Accounting Service core accounting and finance systems, as well as other systems that originate financial transaction data,
- requiring up-front mapping of data flows,
- establishing Memorandums of Agreement between feeder system owners and the Defense Finance and Accounting Service,
- assessing the compliance problem(s),
- developing and implementing corrective action plans,
- requiring end-to-end testing of integrated financial management systems, and
- requiring independent audit verification of compliance.

The process was not formalized until January 2001, and it remains to be seen whether the change of administration will affect its implementation. We continue to believe that it can be an excellent way to coordinate the overall modernization of DoD financial management systems effort.

Logistics. The Deputy Under Secretary of Defense (Deputy Under Secretary) applied Y2K lessons learned, including reusing data from Y2K and partnering with DoD, commercial, and university leaders.

Operational Architecture. The Deputy Under Secretary and the U.S. Transportation Command used the mission-critical threads (thin-lines) that they identified during Y2K end-to-end testing as the foundation for their operational architecture. In addition, the Deputy Under Secretary recaptured the thread information as the first level of data in its modeling and simulation tool called "G2." G2 will use the data to document the baseline for future logistics information technology modernization.

Logistics Integration Center. Through the Y2K end-to-end testing and operational architecture efforts, the Deputy Under Secretary identified the need to review business rules and consider network-centric solutions already in use in commercial industry. The Logistics Integration Center was an initiative to focus on those considerations through partnerships with the Supply Chain

Integration Center, based at the University of Maryland; the Joint Logistics Warfighting Initiative; the Enterprise Integration Center; and other industry leaders, such as Manufacturing Technology, Inc.

Health Affairs. The Assistant Secretary of Defense (Health Affairs) reused data obtained during Y2K and applied lessons learned to configuration management, end-to-end testing, and Memorandums of Agreement.

Change Order Process. The Office of the Assistant Secretary of Defense (Health Affairs) uses the change order process to manage changes to contracts with external business partners. Although the change order process existed prior to Y2K, the Assistant Secretary of Defense (Health Affairs) streamlined the process to support the timelines required by Y2K. The result was a simplified and more direct process that enabled the Military Health System and its contractors to identify needed changes, communicate strategies, develop timelines and expectations, and implement changes in a more timely and effective manner. That streamlined process continued after Y2K and has enhanced communications, cooperation, and the efficiency and effectiveness of changes to information technology throughout the Military Health System.

Configuration Management. The Y2K effort provided a more accurate representation of system configurations through the use of tools such as the Military Health System Integrated Program Planning, Scheduling, and Reporting System, which has been maintained post-Y2K. During the Y2K program, the Military Health System realized that, to reduce vulnerabilities, it needed to increase the information on system software, hardware, and firmware configurations at the site level. The Military Health System carried this Y2K lesson learned forward into its certification and accreditation process by tracking system configurations to ensure that no modifications will affect security accreditation.

End-to-End Testing. The Assistant Secretary of Defense (Health Affairs) conducted end-to-end testing on one of the Military Health System's core systems. Prior to Y2K, system testing included testing only the interface between two systems. However, during Y2K, the interface testing was combined with functional testing of a complete line of interconnected systems to test the functional flow as well as the interfaces and communications systems at the same time.

Memorandums of Agreement. The Medical Treatment Facilities routinely established memorandums of agreement with public and private sector partners to meet a variety of needs. To meet Y2K contingencies, the Medical Treatment Facilities expanded the use of memorandums of agreement to ensure uninterrupted patient care and the continued operation of the facility. In addition, the Military Health System encourages the Military Treatment Facilities to re-evaluate and, when needed, update the memorandums of agreement on an annual basis.

Communications. The Office of the Secretary of Defense (C^3I) applied lessons learned in end-to-end testing. The Joint User Interoperability Communications Exercise is an annual exercise for the Services, Reserve units, and the Defense

Information Systems Agency (DISA). Although the exercise existed prior to Y2K, it had focused only on tactical switches. Since Y2K, the exercise was expanded to focus on the interoperability of the participant's communications systems.

Weapon Systems. The PSA for weapon systems did not retain oversight of Y2K lessons learned applications. The PSA representative provided us with a list of points of contact from Service program executive offices to determine the application of Y2K lessons learned. However, because we focused at the PSA level to determine the application of Y2K lessons learned, we did not extend our audit steps to the Program Executive Office level.

Personnel. The Office of the Under Secretary of Defense (Personnel and Readiness) referenced Y2K efforts and products in the draft Defense Infrastructure Sector Assurance Plan for the Personnel Sector. For example, the plan requires the Personnel Sector to review and update Y2K system contingency plans and thin-line thread plans as appropriate. The plan also requires the Personnel Sector to use mission-critical thin-lines, operational thread plans, Y2K contingency and continuity of operations plans, and Y2K response and recovery criteria for Critical Infrastructure Protection (CIP) purposes.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

Using the relationships established during the Y2K conversion, the ASD(C^3I), as the DoD CIO, continued to foster communications within DoD through the DoD CIO Executive Board, the DoD CIO worldwide conference, and the Information Knowledge Exchange Portal. Additionally, the CIP Directorate under Security and Information Operations adapted Y2K management approaches and concepts in preparing for protection of critical infrastructure. However, in managing other cross-cutting information technology initiatives, the DoD CIO had not taken full advantage of its Y2K experience, as discussed in finding B.

Continued Communications. The DoD CIO fostered communications within DoD, through the DoD CIO Executive Board, the DoD CIO worldwide conferences, and the Information Knowledge Exchange Portal. DoD CIO representatives stated that the Y2K conversion resulted in a greater emphasis for the CIO Executive Board. Additionally, the DoD CIO adapted the Y2K management processes to the DoD CIO Executive Board process. According to DoD CIO representatives, the Board discusses and prioritizes information technology issues similar to the prioritization and discussions of Y2K issues during Senior Steering Group meetings. The DoD CIO also held a worldwide DoD CIO conference in August 2000 and plan to hold another in September 2001. Conferees discuss CIO issues and foster communications among the Office of the Secretary of Defense, the PSAs, the Joint Staff, and Unified Commands. The Information Knowledge Exchange Portal allows users to exchange information using the web. Currently, 150 users have access to the portal, including the DoD CIO Executive Board members, the Office of the

Secretary of Defense, the PSAs, the National Security Agency, and DISA. The portal is intended to facilitate collaboration on policy development and exchange of information. The users can create links to documents, charts, action databases, and calendars to share with other users. The portal contains information on Clinger-Cohen Act compliance, Public Key Infrastructure, and the Global Information Grid.

Critical Infrastructure Protection Plan. The CIP Directorate was adapting Y2K developed management approaches and concepts, such as guidance, thin-lines, exercises, and integration of the warfighter in preparing for protection of critical infrastructure. Critical infrastructure protection ensures the reliability of physical and cyber critical infrastructure. As a result of Y2K, the CIP Directorate developed an operational readiness focused DoD CIP directive. As of August 2001, the CIP Directorate was updating the draft directive based on comments received. Additionally, leveraging Y2K experience, the CIP Directorate was conducting outreach efforts to ensure infrastructure awareness and to create physical and cyber infrastructure thin-lines directly linked to Commander in Chief and Joint Component operational plans and mission requirements. The CIP Directorate also leveraged Y2K operations and consequence management training efforts by integrating CIP related Military Significant Event List items into the Pacific Command Exercise Reception, Staging, Onward Movement, and Integration-00 and the Joint Staff Positive Force-01. A CIP representative stated that physical infrastructure included in the exercises was a result of Y2K. The CIP representative emphasized that an important lesson learned from the Y2K experience was that CIP must address both cyber and physical infrastructure reliability issues and be driven by warfighter mission and capability requirements. In order to integrate the warfighter into the CIP process, the Joint Staff attended the CIP integration staff meetings, that included representatives from all critical infrastructure providers. On December 7, 2000, the ASD(C^3I) reestablished the CIP Directorate and built a management structure under the Deputy Assistant Secretary of Defense for Security and Operations. The Deputy Assistant Secretary of Defense for Security and Operations also serves as the Deputy Critical Infrastructure Assurance Officer.

Director, Operational Test and Evaluation

As described in the Director, Operational Test and Evaluation (DOT&E) FY 2000 Annual Report, DOT&E provided support for Y2K worldwide verification activities, including expert assistance for cross-functional, inter-Service, and cross-system testing. DOT&E also contributed significantly to operational evaluation planning and execution in all of the Unified Commands. Throughout the Y2K operational evaluations, two issues appeared with some regularity: the need for configuration management and the incompletely addressed or unresolved problems with joint interoperability. In addition, organizations had failed to exercise their systems and capabilities to make sure that they worked.

Since the conclusion of the Y2K operational evaluations, DOT&E has continued initiatives resulting from the Y2K work. The DOT&E sponsored representatives at the U.S. European Command, the Joint Forces Command, and United States Forces Korea, who work in areas related to operations planning, command, control, communications, and interoperability. During August 2000, DOT&E sent a team of nine people to support activities of United States Forces Korea's annual Ulchi-Focus Lens 2000 command post exercise. That effort, which used the thin-lines methodology developed for the Y2K operational evaluations, concentrated on activities related to understanding and improving operational processes for preparing target nominations in the development of the Integrated Tasking Order, and on disseminating intelligence with emphasis on requests for information and intelligence summaries.

DOT&E suggested that because the Command, Control, Communication, Computer, and Intelligence infrastructure is in a state of continual change, and because the operational evaluations helped in identifying architectures and thin-line critical systems, DoD should consider institutionalizing periodic operational evaluations that would focus on interoperability once every 3 or 4 years. Such periodic exercises would update the Unified Commands' assessments of their ability to meet mission requirements, allow them to verify the interoperability of existing systems and new programs, and identify those systems that could be eliminated.

Other DoD Components

The Army, Navy, Air Force, National Guard, DISA, and Joint Staff applied lessons learned from Y2K conversion efforts; however, the application varied among and within the DoD Components.

Lessons Learned Applied by the Army. The Director, Information Systems (Command, Control, Communications, and Computers) [The Director], reused the Y2K inventory database as a starting point to determine which Army systems to public key-enable. Public key-enabled applications interoperate with DoD public key infrastructure to access public key certificates and general information in public directories or repositories. Within the Army, the Office of the Deputy Chief of Staff for Personnel Systems of Systems Architecture - Human Resources reused many data elements produced from Y2K to create a database of human resource systems.

Public Key Enabling of Applications. The Director reused the Y2K Army inventory database to assist in developing a list of Army applications to public key-enable. The Y2K inventory database was used to identify all Army mission-critical and mission-essential applications to prioritize which systems to public key-enable.

Personnel Systems of Systems Architecture - Human Resources. The Army Office of the Deputy Chief of Staff for Personnel Systems of Systems Architecture - Human Resources reused the Army Y2K inventory database as a starting point for the Personnel Systems of Systems Architecture - Human Resources web-based database. The system users maintain and update the Y2K data for users to evaluate the impact of a system or procedure change on other systems. The Personnel Systems of Systems Architecture - Human Resources database contains information on Army human resource systems and their interfaces. Reused Y2K system data includes information on hardware, software, thin-lines, and interfaces. Human Resources also reused Y2K manual contingency procedures that were combined with thin-line information to develop diagrams to map the information flow for business processes.

Lessons Learned Applied by the Navy. The Navy CIO reused data collected during Y2K to populate the Navy information technology architecture database. Within the Navy, the Naval Systems Command developed a website for improved configuration management.

Navy Information Technology Architecture Database. The Navy CIO used the Y2K inventory database to populate the Department of the Navy Integrated Architecture Database. The inventory data collected for Y2K was used as a starting point for a complete inventory of applications for the Navy-Marine Corps Internet.

Software Update and Registration Website. The Naval Systems Command applied the Y2K lesson learned of improved configuration management. The Naval Systems Command developed a website for 3,000 users of the software, GateGuard, to obtain the software update and to register that the update was completed. The registration process also resulted in an accurate database of commands and points of contacts. That process has not yet been implemented Navy-wide.

Lessons Learned Applied by the Air Force. The Air Force CIO reused the Y2K inventory database for the Systems Compliance Database and established 11 focus groups to lead key information technology initiatives. The Air Force CFO reused the five-phased approach from Y2K for the CFO process. Within the Air Force, the Deputy Chief of Staff for Installation and Logistics planned to consolidate and reduce the number of logistics systems to achieve improved system management.

System Compliance Database. The Air Force CIO reused data captured in the Air Force Y2K inventory database to populate the System Compliance Database, which is used to better manage information technology investments. The database was expanded to include other data elements and also maintains data captured for Y2K purposes. The Systems Compliance Database tracks systems for section 811 registration; the Air Force-unique Certificate of Networthiness status; Certification and Accreditation status; and the Command, Control, Computers, and Communication systems with the Intelligence Support Plan. Additionally, the database is a management tool for information technology issues such as the Air Force portal and the Global Combat Support Systems framework.

Information Technology Focus Groups. The management process developed to manage the Y2K conversion experience was a positive influence in the development of the focus groups established within the office of the Air Force CIO to manage information technology issues. The 11 focus groups were chartered to lead the way in adopting private industry's best practices for the creation of a network-centric Air Force. Focus areas include the Air Force portal, server consolidation, communications computing transport layer architectures, information assurance architectures, and the Air Force Enterprise Concept of Operations.

Financial System Operations. The Air Force was one of the first DoD Components to adopt the Y2K Management Plan's five-phase process--awareness, assessment, renovation, validation, and implementation--for the improvement of their financial system.

Consolidation of Systems. The Air Force Deputy Chief of Staff for Installation and Logistics issued a memorandum on May 10, 2000, requesting functional managers to consolidate and eliminate systems within a certain timeframe to attain an integrated system for installations and logistics information. The objectives were to better support the warfighter, to streamline and measure the performance of operations, and to reduce the cost of operating information systems. The business process used to handle Y2K events was a driving force behind the logistics policy.

Lessons Learned Applied by the National Guard. The Army National Guard used information from the Y2K inventory database as a starting point in the continued development of the Army National Guard Enterprise Architecture. The systems identified in the inventory, both hardware and software, served as a reference point for determining the function of the operating system currently required within the Army National Guard. Additionally, the Army National Guard uses the inventory information for the continued development of systems by comparing and exploring existing system functions and designs to meet the functional requirements of the users. To better manage its inventory and keep it current, the Army National Guard was developing a web application using the inventory developed during Y2K to identify whether each inventory application was a commercial off-the-shelf, Government off-the-shelf, or an in-house application. The Air National Guard updates the software inventory used during Y2K whenever changes are necessary for software maintenance or upgrades.

Lessons Learned Applied by the Defense Information Systems Agency. DISA reused the Y2K inventory database to develop its technical architecture and interface control documents to identify all interfaces. In addition, DISA annually updates its contingency plans that were developed during Y2K. DISA Western Hemisphere also continues the configuration management efforts that it began for Y2K conversion efforts.

Reusing Inventory. DISA reused the Y2K inventory of applications as a baseline for the development of its technical architecture. The inventory was also used to develop the system's view of DISA architecture, which includes identifying interfaces and components that make up the system. In addition, the Y2K inventory was also incorporated into the DISA Certification and Accreditation process to be used as a system review, which includes the identification of interfaces, the components that make up the system, and the data flow, before the system is accredited.

Updating Interface Control Documents. Reviewing and updating interface control documents were critical to the Y2K process because that process brought about the need for defining interfaces. DISA renewed its effort on the identification of interfaces and, as part of that effort, requires an Interface Control Document as an entrance requirement for any new interface. DISA updates the interface control documents when the interfaces are tested, based on testing results.

Updating Contingency Plans. The Y2K conversion efforts helped DISA to formalize contingency plans for systems. DISA also continues to annually update those contingency plans to include incorporating contingency planning for distributed denial of service attacks through the Internet.

Maintaining Configuration Management. DISA Western Hemisphere continues to maintain two areas of the configuration management database that underwent significant changes during Y2K.

- All associated information about customer application running on the mainframe and the software versions, which run at different locations, proved to be a valuable addition to the inventory and gave the enterprise useful information about the applications.

- DISA Western Hemisphere tracked executive software at a more granular level, including the version levels and vendor patch information, and added tables to associate specific products with customer applications. The information contributes significantly to software optimization and cost savings.

Joint Staff. The Joint Staff published 12 lessons learned in the "Year 2000 Campaign Plan, Volume 1"; however, only 2 of the 12 lessons were adapted. The Joint Staff established CIOs and developed a prototype Joint Operational Architecture. In creating the prototype Joint Operational Architecture, the Joint Staff did reuse some thin-lines developed during Y2K, but it was only a small part of the information used from other sources.

Conclusion

The PSAs, ASD(C^3I), and other DoD Components provided examples of applying Y2K lessons learned. Appendix B provides a more detailed matrix of lessons learned for the following categories: data reuse, adaptation of management experiences, senior management involvement, and continuing partnerships. Appendix C explains these categories and summarizes discussions with DoD Components and PSAs on the lasting impact of Y2K. The DoD Components applied Y2K lessons learned in a variety of ways. However, the DoD CIO did not take full advantage of using Y2K lessons learned to lead the way in managing information technology investments and information assurance.

B. DoD Chief Information Officer Application of Year 2000 Lessons Learned

The DoD Chief Information Officer had not readily adapted its Y2K experiences to managing information assurance and information technology investments. The DoD Chief Information Officer missed opportunities to proactively adapt management approaches, knowledge, and data on systems and interdependencies gained through the Y2K conversion process to managing the security of DoD systems. Additionally, the DoD Chief Information Officer had not shown where Y2K lessons learned were adapted for managing information technology investments, as reported to Congress. As a result, the task of responding to congressional and Office of Management and Budget requirements for ensuring that systems and networks are reasonably secure, particularly with respect to the Government Information Security Reform requirements, and for complying with the Clinger-Cohen Act[1] has been made even more difficult.

Year 2000 Data and Management Experiences

During the process of preparing for Y2K, DoD developed data and processes that were applicable to managing information assurance and information technology investments. However, between January and February 2000, individuals assigned to address the Y2K challenge were released and assigned other duties. Because of the release of these personnel, DoD lost their knowledge and information gained through the Y2K conversion.

Information Assurance. The ASD(C^3I) as the DoD CIO issued the DoD Year 2000 Management Plan to provide a management approach, planning strategy, policy, and actions that enabled DoD to address the Y2K challenge. Additionally, DoD created a database that listed its information technology systems; identified the interfaces between systems; developed thin-lines, which detailed the systems that worked together to complete a particular warfighting mission; and conducted operational evaluations on how processes would continue if key systems failed. Further, the Services and several Defense agencies purchased code-scanning tools.

Information Technology Investments. During the Y2K conversion, DoD Components clearly appreciated the importance of the interoperability of systems and prioritized and invested resources to verify Y2K compliance for the most critical systems and interfaces. DoD Components realized that the inputs, outputs, and interfaces between systems must all work together to successfully perform a mission. DoD used integration testing, continuity of operations

[1] Public Law 104-106, Clinger Cohen Act of 1996, Division E, "Information Technology Management Reform," formally the Information Technology Management Reform Act.

plans, and thin-line architectures to prioritize and manage Y2K compliance efforts within core business and mission areas. The integration testing concentrated on end-to-end testing of business functions and warfighter missions necessary to carry out the national military strategy. DoD used the continuity of operations plans as high level plans designed to ensure that the capability to perform a core mission or function would continue despite disruptions to supporting systems. Thin-line architectures provided insights into warfighting tasks and the reliance on information technology systems. Through these Y2K conversion efforts, DoD senior managers became more aware of the enterprise-wide architectures, missions, business areas, and information technology within DoD.

Information Assurance

The DoD CIO did not take full advantage of Y2K experiences because the DoD CIO missed opportunities to apply lessons learned to information assurance. Several missed opportunities included ensuring the implementation of Joint Staff-developed lessons learned for information assurance, developing overall management guidance for information assurance, reusing the Y2K inventory database to track a system's security status and certification and accreditation date, and renewing licenses for code-scanning tools.

Congressional Report 106-244. In Report 106-244 from the FY 2000 DoD Appropriations Bill, the Committee on Appropriations stated that the steps taken for dealing with the Y2K conversion process were directly related to addressing information assurance. Additionally, the Committee requested a report on lessons learned from Y2K with particular emphasis on what lessons could be applied to information assurance. The ASD(C^3I) report to the congressional Defense committees on Y2K lessons learned, required by Report 106-244, provided the following three statements of lessons learned that the Joint Staff, in coordination with the Unified Commands and other DoD Components, could apply to information assurance.

- Consider databases, thin-lines, and leftover documentation for reuse in information assurance.
- Code-scanning tools had many positive management benefits for future information assurance and information technology initiatives, and DoD would renew licenses for the tools.
- Incorporate information assurance, critical infrastructure protection, interoperability, and configuration management into routine exercises and training.

The Joint Staff representatives did not provide examples that showed lessons learned had been applied.

The ASD(C^3I) report did not state how the DoD CIO would apply Y2K lessons learned to managing information assurance. However, the DoD CIO concluded in the report that "the DoD Y2K effort has laid a firm foundation for longer term improvements in managing and protecting information technology systems…."

Developing Guidance. The ASD(C^3I) as the DoD CIO issued the DoD Year 2000 Management Plan to provide DoD with centralized policy and oversight in preparing for Y2K. The plan included specific procedures for Y2K reporting and certification requirements of DoD Components. The plan also included a description of the five-phase Y2K management process that DoD Components were to use. As discussed in finding A, some PSAs and DoD Components did adapt their Y2K system inventory for managing security certification and accreditation. If the DoD CIO had taken steps to develop guidance on information assurance similar to the procedures in the DoD Y2K Management Plan, clear direction could have been provided for the PSAs and DoD Components and a DoD-wide perspective for tracking security status.

Tracking Security Status. During Y2K, the DoD Y2K office maintained the DoD Y2K database for mission-critical information technology systems to provide the DoD CIO and CIOs of DoD Components with the visibility necessary to ensure a thorough and successful Y2K transition. Each agency reported on the status of its mission-critical systems, including information on the number of systems that were Y2K compliant, being replaced, repaired, and retired. The ASD(C^3I) as DoD CIO used the information to perform oversight and compiled the information for submission to the Office of Management and Budget.

The FY 2001 Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," was promulgated to improve oversight of Federal agency information security programs. Each year, the applicable agency head must submit to the Director, Office of Management and Budget, an assessment of the security program and the systems' security. The Act also requires the Director, Office of Management and Budget, to submit a report to Congress summarizing the information received from each agency.

The DoD CIO should have adapted the Y2K reporting mechanism to oversee compliance with the Government Information Security Reform requirements. The DoD CIO is in the process of responding to the Government Information Security Reform requirements but missed the opportunity to provide a better foundation for managing information security by not readily adapting management experiences and knowledge gained during Y2K conversion.

Tracking Certification and Accreditation. In preparing for Y2K, the DoD CIO tracked the status of the Y2K certification for each system. The DoD Y2K Management Plan required Components to provide the date and level of Y2K certification for mission-critical systems for input into the DoD Y2K database.

DoD Instruction 5200.40, "DoD Information Security Certification and Accreditation Process," December 30, 1997, implements policy, assigns responsibilities, and prescribes procedures for certification and accreditation of information technology, including automated information systems, networks, and sites in DoD. DoD Instruction 5200.40 assigns oversight responsibility to the ASD(C^3I) to ensure that each designated approving authority implements and maintains the DoD Information Technology Security Certification and Accreditation Process for DoD Component and DoD contractor information technology and networks under its jurisdiction.

The DoD CIO could have taken advantage of an opportunity to use the Y2K database as a starting point for overseeing the Certification and Accreditation process required by DoD Instruction 5200.40.

Reusing Y2K Analysis and Renovation Tools. DoD used analysis and renovation tools during Y2K as part of the independent verification and validation process to detect missed date fields and invalid date-processing logic and to validate corrected code. The DoD-provided tools, McCabe Visual 2000 and Mercury Interactive WinRunner 2000, allowed users to analyze programs for errors and to test them after repairs or upgrades were made.

In an August 11, 1999, memorandum, "Use of Department of Defense Provided Tools for Software Testing," the Office of the Assistant Secretary of Defense (C^3I) stated that the McCabe tool could also be used for information assurance. Additionally, DoD Y2K lessons learned reports mentioned the importance of reusing the code-scanning tools. For example, the Air Force report recommended that independent verification and validation procedures become an integral part of configuration management.

The DoD Information Security Certification and Accreditation Process consists of the definition, verification, validation, and the post-accreditation phases. The goal of the verification phase is to produce a fully integrated system ready for certification testing by verifying system compliance with security requirements. The formal certification test and the decision to accredit the system is performed in the validation phase. DoD did not take advantage of reusing code-scanning tools for validation and verification under the DoD Information Security Certification and Accreditation process. Routinely using the DoD-provided tools would significantly enhance DoD software maintenance and quality surveillance efforts in the future. The DoD CIO representatives stated that although the tools were necessary, the Services did not want to fund them and the DoD CIO did not require their use.

Information Technology Investments

The DoD CIO did not take full advantage of Y2K experiences because the DoD CIO missed opportunities to apply lessons learned to information technology investments, particularly with respect to portfolio management. The ASD(C^3I) report to the congressional Defense committees stated that the CIO lessons apply to DoD efforts to achieve compliance with the Clinger-Cohen Act; however, the report did not specify how the DoD CIO planned to use lessons learned to manage information technology investments.

Business or Mission Area Focus. The Y2K conversion process not only drove the identification of individual mission-critical systems and interdependencies, but also resulted in the identification of core business and mission areas. As a consequence, DoD focused Y2K end-to-end testing requirements on the most crucial of operations and business functions and their underlying infrastructure of interconnected systems. The DoD CIO could have used the already identified core processes, missions, and systems in its efforts to manage information technology investments.

Information Technology Investment Management. The Clinger-Cohen Act requires an analysis of the missions and business areas before making significant investments in information technology. That analysis would require an understanding of their underlying portfolios of information technology investments in systems and networks. Additionally, DoD Directive 5000.1, "The Defense Acquisition System," October 23, 2000, states that the acquisition community should adopt "a family-of-systems management approach to ensure that their reviews of individual systems include a thorough understanding of critical system interfaces related to the system under review." DoD Components performed analysis of core business and mission areas and their critical systems and interfaces as part of their Y2K conversion efforts. Also, ASD(C^3I) was developing portfolio management to change the way of investing in information technology systems from focusing on reviews of individual systems to "portfolios" of information technology investments. Portfolios were to be established by grouping information technology investments by mission-related or administrative processes. The ASD(C^3I) representatives envisioned that portfolio management would be an ongoing, collaborative process, performed by stakeholder teams representing all life-cycle activities, and driven by mission outcomes and contribution to the mission. Y2K lessons learned on core business and mission areas and their underlying portfolios of critical systems and interfaces could have been used to formulate an approach to managing information technology investments in a more disciplined manner. However, as of August 2001, the guidance initiated by ASD(C^3I) on portfolio management remained in draft and portfolio management had not yet been implemented by ASD(C^3I).

Information Technology Retirement and Modernization. We asked the DoD Components and PSAs if Y2K aided in accelerating the retirement of legacy systems and in modernizing information technology systems. Several DoD Components and PSAs tracked the accelerated retirement of legacy systems and accelerated modernization of systems. The Army, Air Force, DISA, Army National Guard, and the PSA for Personnel all provided examples of systems retired early because of Y2K. DISA, the Army National Guard, and the PSA for Communications provided examples of systems that were modernized early because of Y2K. According to DoD CIO representatives, many systems were replaced or terminated rather than repaired as a conscious information management strategy. Replacement strategy systems were those that were taken out of the inventory and replaced by one or more existing or new systems prior to January 1, 2000. Termination strategy systems were those that were turned off prior to January 1, 2000. There were 95 mission-critical and 412 nonmission-critical replacement strategy systems and 127 mission-critical and 1,177 nonmission-critical termination strategy systems.

A portfolio approach could continue to help identify modernization needs and retirement or replacement of legacy systems. The Clinger-Cohen Act states that information technology should be evaluated to determine whether to continue, modify, or terminate a program or project. Systems should be retired if their elimination would not disrupt accomplishing a mission, or systems should be replaced if more efficient products exist, such as commercial off-the-shelf products.

Other Uses of Y2K Inventory Database. DoD CIO representatives stated that the Y2K inventory database, now called the DoD Information Technology Registry, was used for the section 811 registration. The DoD CIO representatives mentioned that they could be doing more with the database, in addition to tracking section 811 registration, but had not identified the necessary additional information. For example, the DoD CIO representatives mentioned that the database could track CFO compliance or date-windowing compliance. Date-windowing was used as a temporary solution for Y2K problems by converting 2-digit dates into 4-digit dates when needed. However, date-windowing does not change the 2-digit dates throughout the system's data and will only interpret the date correctly for the appropriate century when used within a certain window of time. When the window expires, the system will interpret dates incorrectly; therefore, the system must be repaired, replaced with new technology, or retired because it is no longer useful. Draft guidance, "Repairing Latent Year 2000 Defects Caused by Date Windowing," was prepared by the Office of the ASD(C^3I). However, as of August 2001 the guidance had not been issued. DoD may lose oversight of the date-windowed systems if guidance is not issued.

Implementing Year 2000 Lessons Learned

In preparing for Y2K, DoD developed complete inventories of information technology. Thin-lines were established, which could have assisted in focusing information assurance requirements on the most critical systems. Contingency plans were prepared or updated to assist in ensuring that processes continued during system failures. End-to-end test plans were available for adaptation to test for identifying information assurance vulnerabilities on systems that were interconnected. This was particularly important because of the interconnection of systems between Services and agencies. Also, core mission and business areas were identified that could have been used in managing information technology investments. The magnitude of the Y2K conversion effort will probably not occur again. Therefore, the DoD CIO must not ignore the benefits of the knowledge and experience gained when managing future information assurance and information technology investments.

Recommendations, Management Comments, and Audit Response

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), as the Chief Information Officer, DoD:

1. Establish a written DoD management plan for information assurance compliance that will oversee the Certification and Accreditation process required by DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997 and that will respond to the requirements of Government Information Security Reform.

Management Comments. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred and stated that the Government Information Security Reform Integrated Process Team was directed to develop a plan for Government Information Security Reform implementation. The second phase of the plan leveraged the assessment mechanism from the Defense Information Technology Security Certification and Accreditation Process.

Audit Response. We consider management comments to be partially responsive. The implementation plan developed by the Government Information Security Reform Integrated Process Team primarily focuses on the Government Information Security Reform requirements for FY 2001. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) should also have a DoD management plan that oversees the certification and accreditation process for information systems and networks, using the DoD information technology registry as a starting point. Accordingly, we request additional comments on a DoD management plan that specifically discusses oversight and guidance on information systems and networks that require certification and accreditation.

2. Assess the cost-effectiveness of purchasing new licenses for analysis and renovation tools to use in detecting defects or abnormalities in software.

3. Implement a mission or business area approach for managing information technology investments in accordance with the Clinger-Cohen Act and DoD Directive 5000.1, "The Defense Acquisition System," October 23, 2000.

4. Implement an oversight process for complete repair, retirement, or replacement of systems that used date-windowing techniques during the year 2000 conversion process.

Management Comments. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with

Recommendations 2., 3., and 4. Management will continue to assess the commercial market for analysis and renovation tools to use in detecting defects or abnormalities in software. Along these lines, management will consider funding a series of studies and publishing guidelines based upon them to assist in determining the best mix of analysis and renovation tools.

The Deputy Chief Information Officer will undertake a thorough review and reengineering of information technology investment and acquisition oversight. The new information technology management and oversight concept includes portfolios and families of systems reviews, which are a mission or business area approach to managing information technology. Other components include mission area management, to direct the mission from an enterprise perspective; investment portfolios and families of systems to maximize total information technology capabilities for mission outcomes; Global Information Grid architecture and implementation to guide the evolution of portfolios and families of systems; families of systems reviews to oversee total information technology and ensure interoperability and architecture; rapid acquisition oversight to speed delivery of effective information technology capabilities to users; and leadership and partnership to establish central guidance with distributed execution. Further, the oversight process for the repair, retirement, or replacement of systems that used date-windowing techniques during the year 2000 conversion process will be included in the family of systems reviews.

Appendix A. Audit Process

Scope

Work Performed. We reviewed and evaluated the application of lessons learned from Y2K within the Office of the DoD CIO, the Services, Joint Staff, DISA, the National Guard, and the PSAs for Health Affairs, Communications, Logistics, Personnel, and Weapon Systems. We focused our review on three main areas: data reuse, management structure and processes, and the continuation of partnerships from the year 2000. We interviewed personnel from each office who were involved with the Y2K conversion and familiar with any application of lessons learned from Y2K, if any. We compared the application of lessons learned among and within each of the Components.

DoD-Wide Corporate Level Government Performance and Results Act Coverage. In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goal and subordinate performance goal.

> **FY 2001 DoD Corporate Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-2)**
>
> **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goal.

Information Technology Management Functional Area.

> **Objective:** Reform information technology management processes to increase efficiency and mission contribution. **Goal:** Institute fundamental information technology management reform efforts. **(ITM-3.2)**

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from December 2000 through May 2001, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did our work in accordance with generally accepted Government auditing standards except that we were unable to obtain an opinion on our system of quality control. The most recent external quality control review was withdrawn on March 15, 2001, and we will undergo a new review. We did not use computer-processed data for this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program Review. We did not review the management control program because we identified no relationship between it and the overall audit objective.

Prior Audit Coverage

General Accounting Office

GAO Report No. AIMD-00-290, "Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges," September 2000

Inspector General, DoD

Inspector General, DoD, Report No. D-2000-041 "Deficiencies in FY 1998 DoD Financial Statements and Progress Toward Improved Financial Reporting," November 26, 1999

Army Audit Agency

Report No. AA-00-214, "Summary of Year 2000 Audit Coverage – Lessons Learned," March 31, 2000

Memorandum Report No. AA 00-90, "Lessons Learned – Year 2000 Audit/Consultation Effort," November 24, 1999

Naval Audit Service

Assessment Report No. N2000-0024, "Y2K Lessons Learned," May 1, 2000

Memorandum: "Lessons Learned From Y2K Conversion," September 30, 1999

Air Force Audit Agency

Memorandum: "Lessons Learned From Y2K Conversion," September 30, 1999

Appendix B. Matrix of Applied Year 2000 Lessons Learned

	Data Reuse								
Agency/ Component PSA	**811 Inventory**	**Other Inventory**	**Thin Lines**	**CP/ COOPs**	**MOAs**	**Adaptation of Y2K Management Experiences**	**Senior Management Involvement**	**Continuing Partnerships**	**Lasting Impact**
ASD (C^3I)	Yes	N/E	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Army	Yes	Yes	Yes	Yes	N/E	N/E	Yes	N/E	Sig
Navy	Yes	Yes	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Air Force	Yes	Yes	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Marine Corps	N/E	N/E	N/E	N/E	N/E	N/E	Yes	N/E	Sig
DISA	Yes	Yes	N/E	Yes	N/E	Yes	Yes	Yes	Mod
Army National Guard	Yes	Yes	N/E	Yes	N/E	N/E	Yes	Yes	Sig
Air National Guard	N/E	Yes	N/E	N/E	N/E	N/E	Yes	N/E	Min
Joint Staff	N/E	N/E	Yes	N/E	N/E	N/E	Yes	N/E	Sig
Health Affairs	Yes	N/E	N/E	Yes	Yes	Yes	Yes	Yes	Sig
Personnel	N/E	Yes	Yes	Yes	N/E	Yes	N/E	Yes	Sig
Com	N/E	N/E	N/E	N/E	N/E	Yes	Yes	Yes	Sig
Logistics	Yes	N/E	Yes	N/E	N/E	Yes	N/E	Yes	Sig
Weapons Systems	N/E	N/E	N/E	N/E	N/E	N/E	N/E	N/E	N/E

Com	PSA for Communications
CP/COOPs	Contingency Plans/Continuity of Operations Plans
Min	Minimal Impact
MOAs	Memorandums of Agreement
Mod	Moderate Impact
N/E	No Evidence provided of lesson learned application
Sig	Significant Impact
Yes	Partial or Overall application of lesson learned

Appendix C. Categories of Lessons Learned and Lasting Impact of Year 2000

Categories of Lessons Learned

Data Reuse. During the audit, we asked the DoD Components and PSAs to provide examples of data collected during the Y2K conversion that proved useful for other purposes and to explain how those data were maintained. Examples of data reuse included system inventories, thin-lines, system contingency plans and organizational continuity of operations plans, and memorandums of agreement. The majority of DoD Components and PSAs stated that they had applied Y2K data to other information technology purposes. For example, the Army, the Joint Staff, and the PSAs for Personnel and Logistics provided examples of reusing Y2K thin-lines. On the other hand, the Marine Corps and the PSA for Communications did not provide examples of data reuse.

Adaptation of Y2K Management Experiences. During the audit, we asked the DoD Components and PSAs to provide examples of Y2K management experiences that had been adapted to other information technology issues. We also asked them to provide examples of end-to-end tests or evaluations performed since the Y2K rollover. Most of the Components and PSAs were able to provide examples of applied Y2K management processes. For example, a DoD CIO representative and the PSAs for Health Affairs, Personnel, Communications, and Logistics provided examples of reusing the Y2K testing structure for other purposes. However, the Army, Marine Corps, National Guard, and Joint Staff did not provide examples for applied Y2K management processes.

Senior Management Involvement. During the course of the audit, we asked the DoD Components and PSAs to discuss the extent to which senior managers and commanders from their respective organizations had remained closely involved in information technology issues since Y2K. The majority of DoD Components and PSAs stated that senior management had remained involved in information technology issues since Y2K. For example, senior management for ASD(C^3I), Air Force, Army, DISA, Joint Staff, and the National Guard attends forums on information technology issues. The PSA for Health Affairs mentioned the high level of involvement in the change order process and the Health Insurance Portability and Accountability. The Navy, Marine Corps, and the PSA for Communications stated that senior management is still involved in information technology issues. On the other hand, the PSAs for Personnel and Logistics stated that senior management involvement is decreasing.

Partnerships. We asked the DoD Components and PSAs if they had continued any of the partnerships with other DoD organizations, Federal agencies, States, and the private sector formed during Y2K. Most DoD Components and PSAs continued partnerships started or strengthened during the Y2K conversion process. DoD CIO representatives, the Navy, and the PSAs for Personnel, Communications, and Logistics, continued to attend forums on information technology issues. DISA Western Hemisphere continued its strengthened relationship with customers. The Air Force continued its partnership with DISA. The PSA for Health Affairs continued partnerships with stakeholders strengthened during Y2K. The National Guard stated that communication improved between the functional and technical personnel. The Army, Marine Corps, and Joint Staff did not provide examples.

Lasting Impact of the Year 2000

During the audit, we asked the representatives from the DoD Components and PSAs how they would characterize the lasting impact of the Y2K conversion on the way that their DoD Component or PSA manages information technology issues. The majority of DoD Components and PSAs characterized the lasting impact of the Y2K conversion process on the way senior management manages information technology issues as significant. For example, the Army, Air Force, and Navy characterized the impact as significant because Y2K increased the awareness of the significance of information technology, especially with senior management. Also, Y2K improved the software development process for the Air Force and increased Navy awareness of the weaknesses in some legacy systems. For the Marine Corps, Y2K improved new system development to prevent stovepipe development. Additionally, the Joint Staff and the PSA for Communications characterized the impact as significant because Y2K improved the modernization of information technology. For DoD CIO representatives, the impact was significant; however, the representatives realized that they missed some opportunities. DISA characterized the impact as moderate since Y2K did not affect the way it manages information technology; however, Y2K did increase awareness of the dependency on information technology. The Air National Guard characterized the impact as minor because it is responsible for only three systems.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense, Deputy Chief Information Officer
Assistant Secretary of Defense (Health Affairs)
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Chief Information Officer, Department of the Army
Inspector General, Department of the Army
Auditor General, Department of the Army
Chief, National Guard Bureau

Department of the Navy

Chief Information Officer, Department of the Navy
Naval Inspector General
Auditor General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Department of the Air Force
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force
Chief, National Guard Bureau

Other Defense Organizations

Director, Defense Finance and Accounting Service
Inspector General, Defense Information Systems Agency

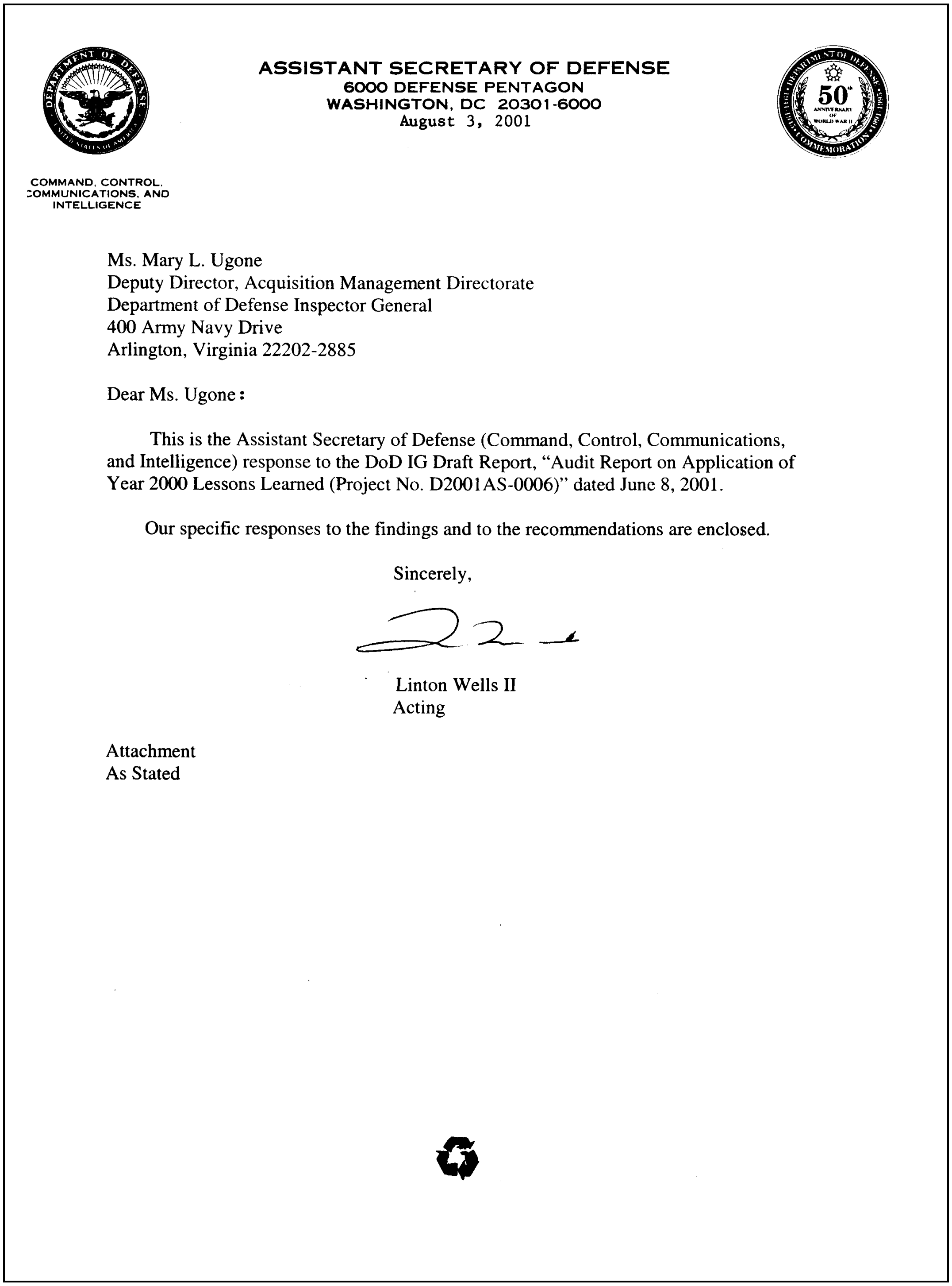
Non-Defense Federal Organizations

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments



ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000
August 3, 2001

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

Ms. Mary L. Ugone
Deputy Director, Acquisition Management Directorate
Department of Defense Inspector General
400 Army Navy Drive
Arlington, Virginia 22202-2885

Dear Ms. Ugone:

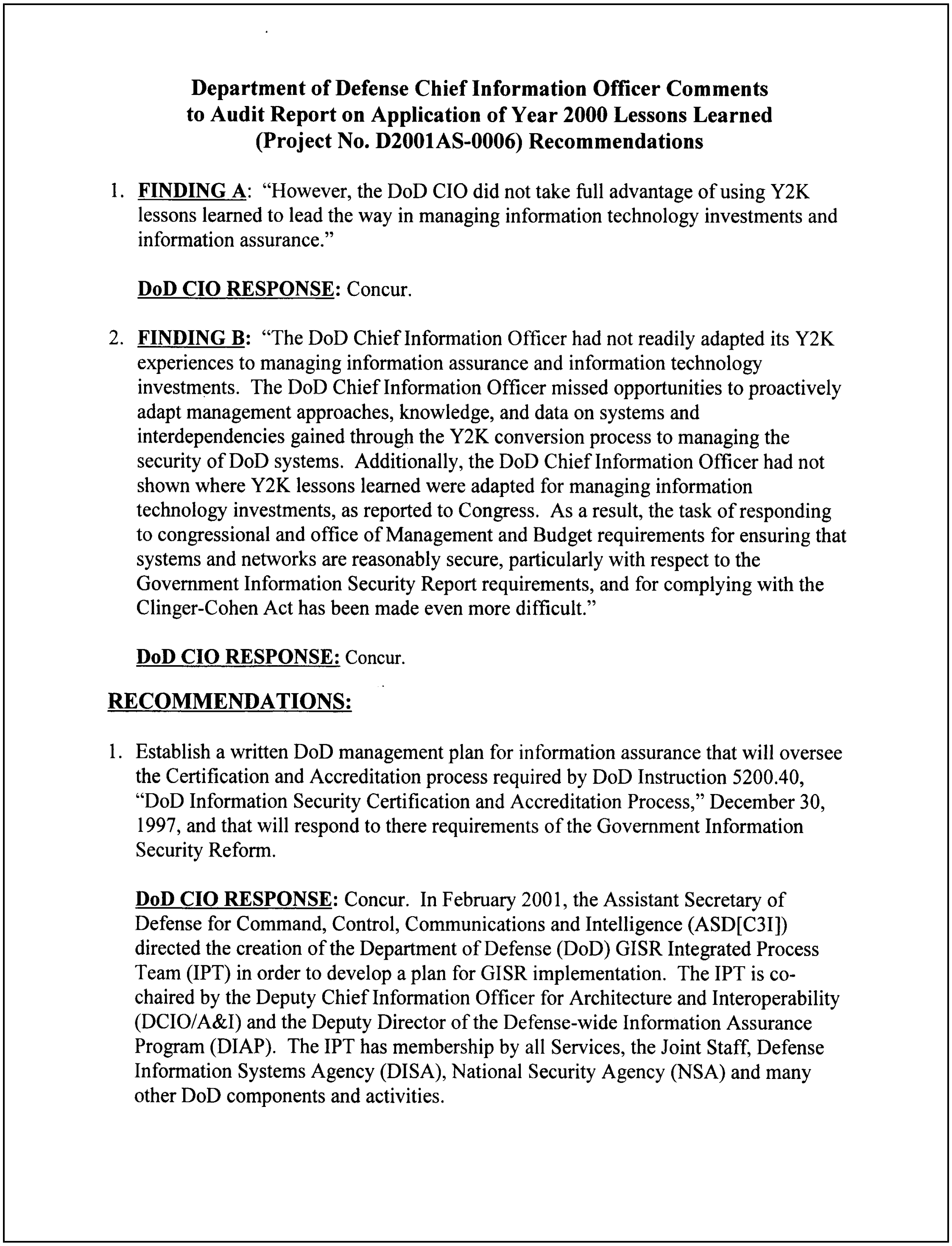
This is the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) response to the DoD IG Draft Report, "Audit Report on Application of Year 2000 Lessons Learned (Project No. D2001AS-0006)" dated June 8, 2001.

Our specific responses to the findings and to the recommendations are enclosed.

Sincerely,

Linton Wells II
Acting

Attachment
As Stated



Department of Defense Chief Information Officer Comments
to Audit Report on Application of Year 2000 Lessons Learned
(Project No. D2001AS-0006) Recommendations

1. **<u>FINDING A</u>**: "However, the DoD CIO did not take full advantage of using Y2K lessons learned to lead the way in managing information technology investments and information assurance."

   <u>DoD CIO RESPONSE</u>: Concur.

2. **<u>FINDING B</u>:** "The DoD Chief Information Officer had not readily adapted its Y2K experiences to managing information assurance and information technology investments. The DoD Chief Information Officer missed opportunities to proactively adapt management approaches, knowledge, and data on systems and interdependencies gained through the Y2K conversion process to managing the security of DoD systems. Additionally, the DoD Chief Information Officer had not shown where Y2K lessons learned were adapted for managing information technology investments, as reported to Congress. As a result, the task of responding to congressional and office of Management and Budget requirements for ensuring that systems and networks are reasonably secure, particularly with respect to the Government Information Security Report requirements, and for complying with the Clinger-Cohen Act has been made even more difficult."

   <u>DoD CIO RESPONSE:</u> Concur.

<u>RECOMMENDATIONS:</u>

1. Establish a written DoD management plan for information assurance that will oversee the Certification and Accreditation process required by DoD Instruction 5200.40, "DoD Information Security Certification and Accreditation Process," December 30, 1997, and that will respond to there requirements of the Government Information Security Reform.

   <u>DoD CIO RESPONSE</u>: Concur. In February 2001, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]) directed the creation of the Department of Defense (DoD) GISR Integrated Process Team (IPT) in order to develop a plan for GISR implementation. The IPT is co-chaired by the Deputy Chief Information Officer for Architecture and Interoperability (DCIO/A&I) and the Deputy Director of the Defense-wide Information Assurance Program (DIAP). The IPT has membership by all Services, the Joint Staff, Defense Information Systems Agency (DISA), National Security Agency (NSA) and many other DoD components and activities.

The DoD GISR plan, as developed by the IPT, incorporates the following three phases:

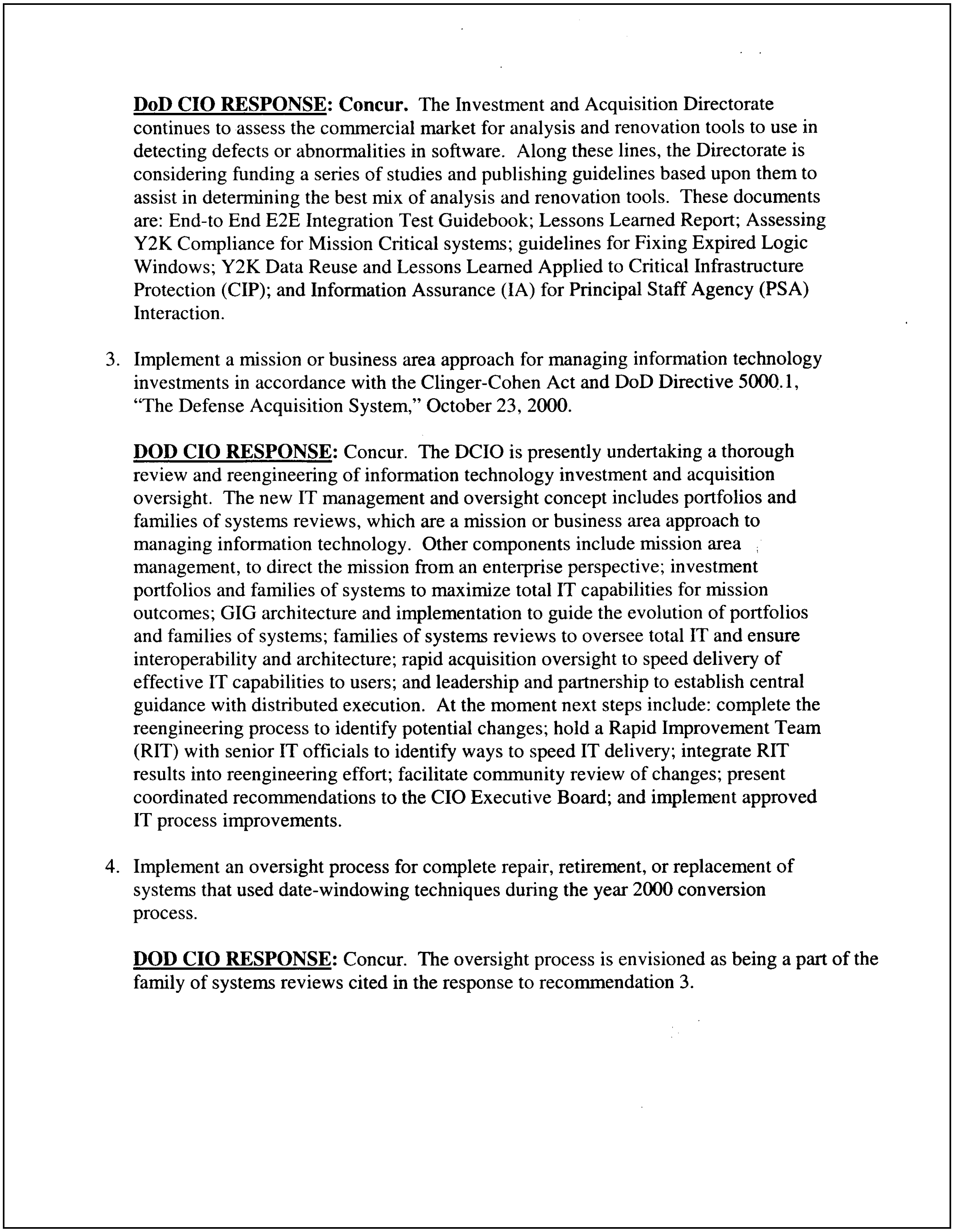
1) Identify a system population and subset for the annual survey
2) Collect information from the DoD Services and Agencies utilizing the GISR Data Collection Matrix
3) Develop annual findings, issues, recommendations and reporting summary to present to the Office of Management & Budget (OMB) for compilation and reporting to appropriate Congressional Committees.

In the first phase, DoD determined that the best measure of the effectiveness of its IA programs and practices would be obtained through assessing the Department's information technology (IT) systems. A measure of a system's performance and IA readiness is a direct reflection on the effectiveness of the IA policies and practices designed to manage it. DoD identified, as its primary systems population, the IT Registry (formerly known as the Y2K Database and 8121 Database). The Registry is divided into three sections based on classification of the systems listed (Unclassified, Secret, Top Secret). DoD will report on Unclassified to non-SCI Top Secret systems and the Intelligence Community CIO will separately report on TS/SCI systems. A statistically valid sample set will be chosen from the Registry systems applicable to DoD and will be sent out to each DoD component and Service to begin GISR data collection.

In the second phase, each DoD component and Service will collect high-level system information using the GISR Data Collection Matrix. The Matrix is designed for aggregate reporting by utilizing pre-defined response format choices. The Matrix was modeled after the National Institute of Standards and Technology (NIST) "Self-Assessment Guide for Information Technology Systems" and assesses, at a corporate level, the selected systems' IA program and practices including access controls, risk management plans, security incident response plans, etc. In addition, DoD leveraged many existing assessment mechanisms, such as the Defense Information Technology Security Certification and Accreditation Process (DITSCAP), Red/Blue teaming, and Information Assurance Vulnerability Alerts (IAVA). By leveraging these existing mechanisms, DoD can successfully tie together disparate, detailed assessments into one complete picture of its IA status and effectiveness.

In the final phase, the DoD CIO will report on its findings and recommendations based on the data collected. This report will be combined with the DoD IG independent evaluation and audit results and then forwarded to OMB. OMB will prepare the Federal GISR report for Congress.

2. Assess the cost-effectiveness of purchasing new licenses for analysis and renovation tools to use in detecting defects or abnormalities in software.



DoD CIO RESPONSE: Concur. The Investment and Acquisition Directorate continues to assess the commercial market for analysis and renovation tools to use in detecting defects or abnormalities in software. Along these lines, the Directorate is considering funding a series of studies and publishing guidelines based upon them to assist in determining the best mix of analysis and renovation tools. These documents are: End-to End E2E Integration Test Guidebook; Lessons Learned Report; Assessing Y2K Compliance for Mission Critical systems; guidelines for Fixing Expired Logic Windows; Y2K Data Reuse and Lessons Learned Applied to Critical Infrastructure Protection (CIP); and Information Assurance (IA) for Principal Staff Agency (PSA) Interaction.

3. Implement a mission or business area approach for managing information technology investments in accordance with the Clinger-Cohen Act and DoD Directive 5000.1, "The Defense Acquisition System," October 23, 2000.

   DOD CIO RESPONSE: Concur. The DCIO is presently undertaking a thorough review and reengineering of information technology investment and acquisition oversight. The new IT management and oversight concept includes portfolios and families of systems reviews, which are a mission or business area approach to managing information technology. Other components include mission area management, to direct the mission from an enterprise perspective; investment portfolios and families of systems to maximize total IT capabilities for mission outcomes; GIG architecture and implementation to guide the evolution of portfolios and families of systems; families of systems reviews to oversee total IT and ensure interoperability and architecture; rapid acquisition oversight to speed delivery of effective IT capabilities to users; and leadership and partnership to establish central guidance with distributed execution. At the moment next steps include: complete the reengineering process to identify potential changes; hold a Rapid Improvement Team (RIT) with senior IT officials to identify ways to speed IT delivery; integrate RIT results into reengineering effort; facilitate community review of changes; present coordinated recommendations to the CIO Executive Board; and implement approved IT process improvements.

4. Implement an oversight process for complete repair, retirement, or replacement of systems that used date-windowing techniques during the year 2000 conversion process.

   DOD CIO RESPONSE: Concur. The oversight process is envisioned as being a part of the family of systems reviews cited in the response to recommendation 3.

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Mary L. Ugone
Wanda A. Hopkins
Virginia G. Rogers
Maria R. Palladino
Melanie Livingston
W. Ryan Pusey